UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/693,605	10/20/2000	Ashraf Madoukh	5009909-6	8437

21129 7590 02/08/2007
SPENCER, FANE, BRITT & BROWNE
1000 WALNUT STREET
SUITE 1400
KANSAS CITY, MO 64106-2140

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	**PAPER NUMBER**
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/693,605	MADOUKH ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 January 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28,40-70,98 and 99* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28,40-70,98 and 99* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

This office action is responsive to Applicant's amendment received on 1/9/2007. Claims 29-39, 71-97, and 100-120 are cancelled. Claims 1-28, 40-70, and 98-99 are pending.

Response to Arguments

Applicant's arguments, see Remarks, on page 12 – Section 2, filed 1/9/2007, with respect to claims 98-99 are persuasive. A new ground(s) of rejection is made with regards to claims 1-28, 40-70, and 98-99 as follow. In response to Applicant's arguments in terms of specific limitations, please note that explanations and citations are provided in paranthesis through out the office action as appropriate.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 40-70 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted step is:

Regarding independent claims 40 and 70, based on the language of the preamble, the essential step of "obtaining/retrieving the encrypted data" is missing.

Regarding to claims 41-66, these claims are rejected on the basis of dependency.

Regarding claims 47, 54, 67, and 69, a "searching" step should be followed by a "retrieving/obtaining" step.

Regarding independent claim 68, based on the language of the preamble, the essential step of "obtaining/retrieving the encrypted data" is missing.

Claims 7-8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is not clear from the language of the whether "a plurality of encryption key identifications" is also used to encrypt a plurality of data entities. For the purpose of examination, Examiner assumes the following language is intended:

The computer readable medium according to claim 1 further comprising:

a plurality of data entities, a plurality encryption keys, and a plurality of encryption key identifications, wherein said plurality of data entities are encrypted by said plurality of encryption keys.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-28 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The database structure, although stored in a computer readable medium, is a non-statutory subject matter because it cannot be categorized under either one of a "process, machine, manufacture, or composition of matter".

Claims 2-27 are rejected on the basis of dependency.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-28, 40-70, and 98-99 are rejected under 35 U.S.C. 102(b) as being anticipated by Akiyama et al., (U.S. Patent No. 6,463,155 and Akiyama hereinafter).

Regarding claims 1, 7, and 28, Akiyama discloses a computer readable medium containing a database structure for storage of encrypted data, the database structure comprising:

at least one data entity (i.e., contents information) encrypted by at least one encryption key (i.e., channel key Kch), the data entity having at least one searchable attribute (i.e., such as channel No. and channel key ID), and at least one encryption key identification (i.e., channel number) stored in association with the data entity and corresponding to the encryption key (i.e., each channel No. corresponds to a channel key Kch)(col. 9, lines 54-64).

Regarding claim 40, Akiyama discloses method for storage and retrieval of encrypted data, the method comprising:

encrypting a data entity with an encryption key (i.e., channel key Kch) having an encryption key identification (i.e., channel number), storing the data entity, and storing the encryption key identification in association with the data entity (i.e., contents information of each channel is stored in the contents information database 21)(col. 9, lines 54-64).

Regarding claim 68, Akiyama discloses a method for retrieval of encrypted data at rest, the method comprising:

requesting a data manipulation using a searchable attribute, searching a plurality of data entities for matches to the searchable attribute, obtaining an encryption key

identification from the data entities (col. 9, lines 1-9), searching for an encryption key using the encryption key identification, and decrypting the data entities with the encryption key (col. 41, lines 15-36).

Regarding claim 70, Akiyama discloses a method for storage and retrieval of encrypted data, the method comprising:

encrypting a plurality of data entities with a rotating and dynamic encryption key having an encryption key identification, storing the data entities, and creating and rotating to a new encryption key upon occurrence of a desired rotation event (col. 9, lines 10-47).

Regarding claim 98, Akiyama discloses a method of providing a secure environment for the storage of information, the method comprising:

encrypting a data entity with an encryption key (i.e., channel key Kch) having a randomly generated encryption key identification (i.e., channel number), storing the data entity, and storing the encryption key identification in association with the data entity (i.e., contents information of each channel is stored in the contents information database 21)(col. 9, lines 54-64).

Regarding claims 2, 5, and 99, Akiyama discloses wherein the at least one encryption key identification is encrypted by a system key (i.e., master key Km), and the database structure further comprises a system key common name corresponding

to the system key (i.e., seed ID), the system key common name being stored in association with the data entity (col. 8, lines 50-54).

Regarding claims 6 and 8, Akiyama discloses wherein the plurality of encryption keys comprises dynamic encryption keys, and the plurality of encryption key identifications comprise dynamic encryption key identifications (i.e., channel keys and their corresponding channel numbers are said to be dynamic based on the contract period)(col. 9, lines 1-28).

Regarding claim 9, Akiyama discloses wherein the data structure further comprises a plurality of hash values with each of the searchable attributes having a corresponding hash value (col. 45, lines 23-37).

Regarding claim 10, Akiyama discloses wherein the data structure further comprises at least one integrity attribute in association with the data entity (col. 23, lines 40-44 and col. 32, lines 1-52).

Regarding claim 11, Akiyama discloses wherein the data structure further comprises a security key attribute of the data entity, the security key attribute including the at least one encryption key identification and a system key common name (col. 8, lines 50-57).

Regarding claims 12, 63 and 65, Akiyama discloses wherein the data entity and encryption key identification are stored in a first database, and further comprising storing the encryption key in a second database (i.e., contents information database 21 contains the contents information corresponding to each channel number while channel key database 4 stores the channel key)(col. 9, lines 54-64).

Regarding claim 13, Akiyama discloses wherein the first database further includes a system key common name stored thereon, and the system key common name corresponds to a system key used to encrypt the encryption key identification (i.e., master key Km is used to encrypt the appending information)(col. 10, lines 58-65).

Regarding claim 14, Akiyama discloses further comprising a security token including the system key stored thereon (col. 22, lines 39-60 – wherein seed database entry is recorded in a card shaped recording medium).

Regarding claim 15, Akiyama discloses wherein the security token comprises a Smart Card reader (col. 22, lines 39-60 – wherein seed database entry is recorded in a card shaped recording medium).

Regarding claim 16, Akiyama discloses wherein the at least one encryption key identification (i.e., channel No.) is stored as an attribute of the data entity (i.e., fields of database entries)(Figs. 3-4 and 6 and their corresponding text).

Regarding claim 17, Akiyama discloses wherein the data entity comprises a data object (i.e., database entries) having a plurality of attributes (i.e., fields of database entries)(Figs. 3-4 and 6 and their corresponding text).

Regarding claim 18, Akiyama discloses further comprising a second data entity including as attributes the encryption key and the encryption key identification (i.e., channel key database entry includes channel No. and channel key fields)(Fig. 6 and its corresponding text).

Regarding claim 19, Akiyama discloses wherein the second data entity is stored on a separate isolated database from the at least one data entity (i.e., fields of different database entries are retrieved from separate databases such as contracting user database, seed database, and channel key database)(Fig. 3-6 and their corresponding text).

Regarding claim 20, Akiyama discloses further comprising a second data entity encrypted by a second encryption key, the second data entity having a second searchable attribute, and a second encryption key identification corresponding to the second encryption key, and wherein the at least one encryption key comprises a first encryption key and the at least one encryption key identification comprises a first encryption key identification (i.e., since channel key changes periodically, channel

related appending information (element of Fig. 13 – equivalent to a first data entity), changes accordingly to accommodate for decryption of the contents information in conjunction with the channel key change – wherein the second version of channel related appending information corresponds to the second data entry)(col. 13, lines 65-67 and col. 14, lines 1-14).

Regarding claim 21, Akiyama discloses wherein the second encryption key identification is stored as an attribute of the second data entity (col. 22, lines 1-7).

Regarding claim 22, Akiyama discloses wherein the first and second encryption key identifications are encrypted by a system key (i.e., master key Km) having a system key common name (i.e., seed ID)(col. 8, lines 50-54).

Regarding claim 23, Akiyama discloses wherein the system key comprises a public system key (col. 33, lines 29-36).

Regarding claim 24, Akiyama discloses further comprising the system key common name stored as an attribute of the first and second data entities (col. 8, lines 50-54 – two seed database entries with different validity periods with different seed Ids – Fig. 5).

Regarding claim 25, Akiyama discloses wherein the first encryption key identification is encrypted by a first system key, and the second encryption key identification is encrypted by a second system key (i.e., master key Km is generated using the random number generation and the encryption algorithm and is stored in the memory indicated by the master key identifier ("0" or "1" of the relative ID)(col. 28, lines 53-61 and col. 29, lines 56-67 and col. 30, lines 1-6).

Regarding claim 26, Akiyama discloses wherein the first and second data entities contain information for an individual customer (i.e., the reception device ID)(col. 30, lines 19-33).

Regarding claim 27, Akiyama discloses wherein the first data entity contains medical patient name information, and the second data entity contains medical patient address information (i.e., depending on the content of the database, any information can well be queried from the database wherein the result of such queries are presented in the form of first, second, and ... data entries. Therefore, the contents of such data entities are design and application choices and are not considered novelty).

Regarding claim 41, Akiyama discloses further comprising:

requesting a data manipulation using a searchable attribute, searching for matches to the searchable attribute, searching for the encryption key using the

encryption key identification, and decrypting the data entity with the encryption key (col. 9, lines 1-9 and col. 41, lines 15-36).

Regarding claim 42, Akiyama discloses wherein requesting the data manipulation comprises requesting a data update of new information (col. 7, lines 17-42 and col. 18, lines 50-63), and further comprising encrypting the new information with a second encryption key (col. 9, lines 29-53).

Regarding claim 43, Akiyama discloses wherein requesting the data manipulation comprises requesting an addition of new information (col. 7, lines 17-42 and col. 18, lines 50-63), and further comprising encrypting the new information with a second encryption key (col. 9, lines 29-53).

Regarding claim 44, Akiyama discloses wherein requesting the data manipulation comprises requesting viewing of current information (col. 7, lines 17-42 and col. 18, lines 50-63), and further comprising encrypting the viewed information with a second encryption key (col. 9, lines 29-53).

Regarding claim 45, Akiyama discloses further comprising encrypting the encryption key identification with a system key having a system key common name (i.e., seed ID)(col. 8, lines 50-54).

Regarding claim 46, Akiyama discloses further comprising storing the system key in a security token (col. 22, lines 39-60 – wherein seed database entry is recorded in a card shaped recording medium).

Regarding claim 47, Akiyama discloses further comprising:

requesting a data manipulation using a searchable attribute, searching for matches to the searchable attribute, searching for the system key using the system key common name, decrypting the encryption key identification with the system key, searching for the encryption key using the encryption key identification, and decrypting the data entity with the encryption key (col. 9, lines 1-9 and col. 41, lines 15-36).

Regarding claim 48, Akiyama discloses wherein encrypting the encryption key identification with a system key comprises encrypting the encryption key identification with a system public key (col. 33, lines 29-36).

Regarding claim 49, Akiyama discloses further comprising decrypting the encryption key identification with a system private key (col. 33, lines 29-36).

Regarding claims 50 and 53, Akiyama discloses further comprising encrypting the encryption key identification with a system key having a system key common name, hashing the system key common name to create a system key common name hash

value, and storing the system key common name and system key common name hash value in association with the data entity (i.e., master key Km is used to encrypt the appending information)(col. 10, lines 58-65) Akiyama discloses the encrypted reception contract information or its hash value can be applied with digital signature as authentication information. Akiyama uses hash values to express data of arbitrary length in a given length (col. 45, lines 23-37).

Regarding claims 51-52 and 56, Akiyama discloses further comprising checking for expiration of the system key, and upon expiration of the system key, discontinuing use of the system key and generating and using a new system key (col. 24, lines 1-20).

Regarding claim 54, Akiyama discloses further comprising:

requesting a data manipulation using a searchable attribute, searching for matches to the searchable attribute, searching for the system key common name using the system key common name hash value, searching for the system key using the system key common name, decrypting the encryption key identification with the system key, searching for the encryption key using the encryption key identification, and decrypting the data entity with the encryption key (col. 9, lines 1-9 and col. 41, lines 15-36 and col. 10, lines 58-65).

Akiyama discloses the encrypted reception contract information or its hash value can be applied with digital signature as authentication information. Akiyama uses hash values to express data of arbitrary length in a given length (col. 45, lines 23-37).

Regarding claim 55, Akiyama discloses further comprising verifying the system key with a private certificate authority, and performing an integrity check on the system key (col. 32, lines 53-67 and col. 33, lines 1-36).

Regarding claim 57, Akiyama discloses further comprising upon expiration of the encryption key, generating a new encryption key having an expiration date, retrieving data entities using the encryption key (col. 15, lines 40-60), decrypting the retrieved data entities with the encryption key, encrypting the retrieved data entities with the new encryption key, storing the retrieved data entities (col. 18, lines 17-64).

Regarding claim 58, Akiyama discloses further comprising hashing searchable attributes of the data entity to determine data entity attribute hash values and storing the data entity attribute hash values in association with the data entity. Akiyama discloses the encrypted reception contract information or its hash value can be applied with digital signature as authentication information. Akiyama uses hash values to express data of arbitrary length in a given length (col. 45, lines 23-37).

Regarding claim 59, Akiyama discloses further comprising:

requesting a data manipulation using a searchable attribute, hashing the searchable attribute to create a searchable attribute hash value, searching for matches to the searchable attribute hash value, searching for the encryption key using the

encryption key identification, and after retrieving the encryption key, decrypting the data entity with the encryption key (col. 17, lines 55-64). Akiyama discloses the encrypted reception contract information or its hash value can be applied with digital signature as authentication information. Akiyama uses hash values to express data of arbitrary length in a given length (col. 45, lines 23-37).

Regarding claim 60, Akiyama discloses further comprising transmitting the data entity over a data transmission line, and wherein encrypting the data entity comprises encrypting only a portion of the data entity in accordance with a business rule (i.e., only the contents information is encrypted using channel key Kch which is reception device specific and gets updated/managed based on the reception contract/business rule which defines whether or not a reception device may be able to view/access contents information)(col.18, lines 17-64).

Regarding claims 61-62, Akiyama discloses further comprising generating a new encryption key for each user action (i.e., new subscription or change of the contract content)(col. 37, lines 19-47 and col. 40, lines 10-17) .

Regarding claim 64, Akiyama discloses further comprising auditing the encryption key for a desired event (i.e., upon receiving the terminal related appending information at the reception device)(col. 12, lines 51-67).

Regarding claim 66, Akiyama discloses further comprising encrypting the encryption key identification with a system key having a system key common name, and maintaining the system key within a security domain at all times (i.e., the security domain is controlled by the public key cryptosystem)(col. 33, lines 9-36)

Regarding claim 67, Akiyama discloses further comprising:

requesting a data manipulation using a searchable attribute, searching for matches to the searchable attribute, searching for the encryption key using the encryption key identification (col. 9, lines 1-9 and col. 41, lines 15-36), performing an integrity check on the encryption key, and decrypting the data entity with the encryption key (col. 33, lines 9-36).

Regarding claim 69, Akiyama discloses further comprising:

obtaining a system key common name from the data entities, searching for a system key using the system key common name, decrypting the encryption key identification with the system key (i.e., the appending information includes the encryption key identification)(col. 17, lines 60-64).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3-4, 9, 53-54, and 58-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Akiyama et al., (U.S. Patent No. 6,463,155 and Akiyama hereinafter), in view of Mansfield, Jr. et al., (U.S. Patent No. 5,530,939 and Mansfield hereinafter).

Regarding claims 3-4, 9, 53-54, 58-59, with respect to disclosing hash value of the searchable attribute, Akiyama discloses the encrypted reception contract information or its hash value can be applied with digital signature as authentication information. Akiyama uses hash values to express data of arbitrary length in a given length (col. 45, lines 23-37).

Akiyama does not expressly disclose searching and retrieval of searchable hash values.

However, Mansfield discloses to include query execution using hash partitioning (col. 20, lines 15-67 and col. 21, lines 1-30).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Akiyama with teachings of Mansfield because it would allow to include query execution using hash partitioning with the motivation to allow concurrent execution of queries in a much more efficient manner (Mansfield, col. 20, lines 1-3).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Linehan et al., (U.S. Patent No. 5,495,533),

Ginter et al., (U.S. Patent No. 6,640,304),

Al-Salqan, (U.S. Patent No. 6,160,891),

Matyas, Jr. et al., (U.S. Patent No. 6,947,556), and

Dolan et al., (U.S. Patent No. 5,604,801).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Arezoo Sherkat
Patent Examiner
Group 2131
Feb. 1, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100